AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with
runningparrots@googlemail.com that is stored at
premises controlled by Google, Inc.

Case No. 13-m-228

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

□ evidence of a crime;

□ contraband, fruits of crime, or other items illegally possessed;

□ property designed for use, intended for use, or used in committing a crime;

□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1037(a)(3) and 1030	The CAN-SPAM Act and fraud and related activity in connection with computers.

The application is based on these facts:
See attached affidavit.

☑ Continued on the attached sheet.

□ Delayed notice of _____ days (give exact ending date if more than 30 days: ____________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Richard H. Bilson, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: April 5, 2013

Patricia J. Gorence
Judge's signature

City and state: Milwaukee, Wisconsin

Patricia J. Gorence
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with runningparrots@googlemail.com that is stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheater Parkway, Mountain View, California, 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on March 15, 2013, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including Web history, address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of CAN-SPAM Act, 18 U.S.C. § 1037(a)(3), and fraud and related activity in connection with computers, 18 U.S.C. § 1030, those violations involving an unknown individual using the email address runningparrots@googlemail.com and jabber account casesensitive@jabber.org and occurring after February 18, 2012, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications and websites related to the registration of Internet domains.

b. Communications and websites related to malware and/or computer viruses.

c. Communications websites related to computer botnets.

d. Communications and websites related to financial transactions.

e. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Richard H. Bilson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with an account that is stored at premises controlled by Google, Inc., an e-mail provider headquartered at 1600 Amphitheater Parkway, Mountain View, California, 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since January of 2010. I am currently assigned to the FBI Milwaukee Division's Computer Intrusion Task Force. As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. In this role, I have investigated numerous criminal and national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of personally identifiable information, and other computer related fraud. Prior to becoming a Federal Agent, I worked in a variety of public and private positions in the Information Technology industry. I have also received training in computer technology,

computer fraud, and have held industry certifications from Microsoft, Novell, Cisco, and CompTIA.

3. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of CAN-SPAM Act, 18 U.S.C. § 1037(a)(3), and fraud and related activity in connection with computers, 18 U.S.C. § 1030 have been committed by unknown persons using email address runningparrots@googlemail.com. There is also probable cause to search the information described in Attachment A for evidence or instrumentalities of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

6. Based on my training and experience, I am aware that:

a. A "bot" is a computer that contains a software program that interacts with network services intended for people as if it were a person. The term is derived from "robot." There are both illegal and legal uses for a bot. However, in this investigation, a bot is malicious in that it is used to send and receive commands on computers that have been illegally compromised.

b. A "botnet" is a collection of software robots, or bots, which run autonomously. The term is derived from "robot network." Botnet is generally used to refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure. A botnet's originator (a.k.a. "botherder") can control the group remotely through various means and usually for nefarious purposes. Botnets serve various criminal purposes, including launching and controlling denial-of-service attacks, creating and misusing Simple Mail Transfer Protocols (SMTP) mail relays or proxies for spam, click fraud, and the theft of personal identifying information.

c. The Domain Name System (DNS) is a naming system for computers connected to the Internet. An often-used analogy to explain DNS is that it serves as a phone book for the Internet by translating easily memorized domain names such as "anymachine.anydomain.com" into IP addresses such as 192.168.1.1.

d. A "fast fluxing botnet" is a DNS technique used by botnets to obfuscate phishing and malware delivery sites behind an ever changing network of bots acting as proxies. The basic premise of fast flux is to associate numerous IP addresses with a single domain, where IP addresses are swapped in and out with extremely high frequency, through changing DNS records. This process completely obfuscates the actual IP addresses being used to conduct illegal activities.

e. Bullet Proof hosting (BP) is a term used for a web hosting provider that will host virtually any content, from phishing and carding sites to botnet command centers and Internet browser exploit kits.

f. Phishing is an attempt to obtain financial or other confidential information from Internet users, typically by sending an e-mail that looks as if it is from a legitimate organization (frequently a financial institution), but which contains a link to a fake Web site that replicates the real one.

g. ICQ is an instant messaging computer application that allows a user to chat online in real time with other users through various client applications. ICQ uses a unique identification number (UIN) to identify each user that utilizes the ICQ service. ICQ is currently owned and operated by Digital Sky Technologies.

h. Jabber is an instant computer application that allows a user to chat online in real time with other users through various client applications.

PROBABLE CAUSE

7. On November 1, 2012, a FBI confidential human source (CHS1) identified multiple advertisements placed by an individual using the online moniker "casesensitive," on several Internet forums. The following advertisement was posted by casesensitive on the Internet forum Lampeduza.com on October 25, 2012: "Hey guys, we are pleased to inform you

that we are selling very fast botnet hosting and dedicated servers. Anyone interested PM (Private Message) me for a demo or more info." The advertisement also included the ICQ number 602580050.

8. Based on this advertisement, CHS1 contacted casesensitive via ICQ and explained he was interested in bullet proof hosting. Casesensitive advised CHS1 that he could provide hosting on a botnet with dual fast fluxing capability which included DNS on bots and 99% uptime. CHS1 requested casesensitive's jabber ID so their communications could be more secure. Casesensitive advised his jabber ID was casesensitive@jabber.org.

9. CHS1 then contacted casesensitive via jabber. CHS1 asked if would be possible to host phishing on his botnet. Casesensitive replied he would host anything except for child pornography. CHS1 then requested a demonstration of the functionality of the botnet and provided an image and a line of text to casesensitive. Casesensitive provided the URL http://abc.himpi.com to CHS1 for the botnet demonstration. When clicked, the CHS was presented with a web page which contained the image and text that had previously been sent to casesensitive by CHS1, thus demonstrating casesensitive's ability to host a webpage containing whatever content CHS1 asked for (including websites which appeared to be legitimate financial institution websites).

10. A lookup of the domain http://abc.himpi.com revealed it was currently resolving to multiple IP addresses. A second lookup of the same domain several minutes later revealed it was resolving to multiple IP addresses which differed from the initial lookup, thus validating the fast fluxing functionality of the botnet. Casesensitive advised CHS1 that it would cost $550 per month for shared hosting (single server hosting multiple clients) and $1,600 per month for dedicated hosting (single server for one client) with a dedicated DNS domain.

11. On November 6, 2012, an FBI Special Agent, acting in an online covert capacity (OCE-4583), conducted the following consensually monitored conversation with an individual who utilized the online moniker casesensitive@jabber.org. During conversation, OCE-4583 inquired about purchasing bullet proof hosting from casesensitive@jabber.org to host a phishing site. Casesensitive advised that he/she could provide hosting utilizing a botnet with fast flux capabilities. The following in an excerpt of the conversation between casesensitive@jabber.org and OCE-4583 on November 6, 2012, at 9:15:29 AM CST:

```
(12:26:34 PM) OCE: hi
(12:27:08 PM) Attempting to start a private conversation with
casesensitive@jabber.org...
[Image] (12:27:12 PM) Unverified conversation with
casesensitive@jabber.org/24425ce3be2e6f40 started. Your client is logging this
conversation.
(12:30:25 PM) casesensitive@jabber.org: hello
(12:30:25 PM) casesensitive@jabber.org: sup
(12:31:46 PM) OCE: hi what can u do for us
(12:31:59 PM) OCE: we need backup bp [bulletproof hosting][1]
(12:32:38 PM) OCE: ned to test again i didnt see
(12:33:50 PM) casesensitive@jabber.org: sec
(12:33:55 PM) casesensitive@jabber.org: ill put up the site for u
(12:34:19 PM) OCE: kk
(12:39:38 PM) casesensitive@jabber.org: http://abcd.himpi.com/
(12:58:30 PM) OCE: wher main server if we buy dedicated
(12:58:39 PM) casesensitive@jabber.org: main server is US
(12:58:41 PM) casesensitive@jabber.org: 1gbit port
(12:59:07 PM) OCE: nice
(12:59:21 PM) OCE: how $?
(1:00:07 PM) casesensitive@jabber.org: shared or dedicated
(1:00:08 PM) casesensitive@jabber.org: ?
(1:00:18 PM) OCE: dedicate
(1:00:27 PM) casesensitive@jabber.org: btw in this demo domain
(1:00:33 PM) casesensitive@jabber.org: i've banned RU [Russia]
(1:00:34 PM) casesensitive@jabber.org: :p
(1:00:39 PM) casesensitive@jabber.org: so u wont be able to access domain from RU
(1:00:51 PM) casesensitive@jabber.org: RU, RO, CN [Russia, Romania, China]
```

[1] The bracketed information is an explanation of abbreviations and was not part of the conversation.

(1:01:08 PM) OCE: ok

(1:01:34 PM) OCE: i was able to open site

(1:01:45 PM) OCE: im not from ru ip

(1:01:49 PM) casesensitive@jabber.org: okie :)

(1:02:25 PM) casesensitive@jabber.org: shared is 550 a month. dedicated is 1600 a month. we will give u 2 dns domains as well. uptime is better than chinese or other servers :) ull feel the difference in all ways.. speed uptime

(1:02:48 PM) casesensitive@jabber.org: and we have ddos protection as well - ill add tht plugin to ur server for free as u will be a new client

(1:02:58 PM) OCE: china sucks we use eu servers

(1:03:16 PM) casesensitive@jabber.org: u dont need to worry on seerver being shut down at all

(1:03:30 PM) casesensitive@jabber.org: **no one is able to track real server so its protected** :)

(1:04:14 PM) OCE: wher dns at

(1:04:40 PM) casesensitive@jabber.org: **bots :)**

(1:09:03 PM) OCE: kk

(1:11:01 PM) OCE: how accept $

(1:11:30 PM) casesensitive@jabber.org: wmz ? [Webmoney, a Russian-based electronic money and online payment system]

(1:12:57 PM) OCE: dont use wmz anymore, LR? [Liberty Reserve, a Costa Rican-based electronic money and online payment system]

(1:14:22 PM) OCE: **what kind of sites u host normally**

(1:14:33 PM) casesensitive@jabber.org: sure i can do LR too

(1:14:50 PM) casesensitive@jabber.org: **pharma, adult, casino**

(1:15:02 PM) casesensitive@jabber.org: hosted sendsafe in the past too

(1:15:42 PM) OCE: cool

(1:31:07 PM) OCE: if we buy share how many share server

(1:33:04 PM) casesensitive@jabber.org: around 5-6

(1:33:45 PM) casesensitive@jabber.org: and each client has his big chunk of domains

(1:33:47 PM) OCE: how affect speed

(1:34:13 PM) casesensitive@jabber.org: speed is divided among traffic coming in.. if u need best speeds

(1:34:16 PM) casesensitive@jabber.org: u need dedicated

(1:34:41 PM) casesensitive@jabber.org: but some guys are doing facebook on shared too.. so their traffic comes insane too

(1:36:17 PM) OCE: any phishing on share server

(1:39:47 PM) OCE: ?

(1:41:47 PM) casesensitive@jabber.org: **yes clients do host phish**

(1:41:53 PM) casesensitive@jabber.org: but no child porn allowed

(1:46:15 PM) casesensitive@jabber.org: im sure when u will start using this server as a backup server. u will change ur mind and make it as ur primary server :)

(1:47:24 PM) OCE: k will talk to partner all looks good need to decide share or dedicated

(1:47:36 PM) casesensitive@jabber.org: okie sure

12. While conducting the consensually monitored conversation above, OCE-4583 repeatedly conducted domain lookup requests for the domain name http://abcd.himpi.com, provided by casesensitive. The following is a list of IP addresses associated with said domain name:

98.222.107.196
96.28.48.222
94.8.124.243
90.217.141.56
89.229.0.121
89.206.2.127
88.234.142.58
88.226.230.31
88.224.200.16
87.120.210.203
86.210.240.198
85.240.0.95
81.61.217.85
78.98.69.127
77.88.150.163
77.127.127.140
77.125.138.170
75.118.192.224
74.15.149.82
71.58.235.76
71.236.22.107
71.228.135.174
71.178.27.180
69.251.60.186
68.57.226.36
67.184.74.33
50.90.225.173
50.140.199.125
46.2.181.246
46.12.174.196
41.92.42.182
41.185.110.23
31.53.58.215
27.106.115.51
24.2.231.76
24.14.202.182
213.238.112.99
210.125.91.96
200.56.144.77
195.116.59.10
190.58.224.20
190.150.54.136
189.194.233.228
189.153.172.97
186.104.175.252
184.14.166.2
183.82.164.34
183.82.162.82
183.82.162.82
181.129.160.14
176.44.2.124
176.35.199.252
174.114.121.109
151.62.18.117
149.241.235.228
121.175.172.173
109.11.171.175
108.50.177.142
108.132.223.56

13. Based on my training and experience, I am aware that associating multiple IP addresses with a single domain and swapping the IP addresses in and out with extremely high

frequency is indicative of a fast fluxing botnet. This process completely obfuscates the actual IP addresses being used to conduct illegal activities.

14. On November 12, 2012, CHS1 requested casesensitive provide additional contact information for future contact. Casesensitive responded to CHS1 with the following information: "icq 602580050, jabber casesensitive@jabber.org, email runningparrots@googlemail.com".

15. An open source query of the email address runningparrots@googlemail.com revealed this email address was used to register the domains m1k.in on February 19, 2012, and c81.in on March 28, 2012. Additional investigation revealed that some of the IP addresses identified during the fast fluxing botnet demonstration resolved to these two domains.

16. Additionally, open source queries revealed that over 3,600 IP addresses resolved to the domain m1k.in and over 1,200 IP addresses resolved to c81.in since the initial domain registrations. Based on additional database records obtained, queries of the IP addresses identified herein revealed a total of 15 Internet domains and 8,464 unique IP addresses were used by the botnet run by casesensitive in 2012 and 2013, including IP addresses that are registered to computers in the Eastern District of Wisconsin.

17. On January 17, 2013, this Court ordered the installation of pen register and trap and trace devices on the Jabber (instant messaging) account casesensitive@jabber.org to collect IP addresses used to access the account. On March 20, 2013, Google responded to a subpoena dated February 15, 2013, with subscriber and IP address information for runningparrots@googlemail.com. The IP address used to access the email account on February 1, 2013, is the same IP address used to access the jabber account during the time period of January 22, 2013, to February 20, 2013. According to the information from Google, I am aware

that the user for this email account also uses the following other Google Services: Blogger, Gmail, Google Drive, Google Talk, Google Webmaster Tools, Google+, Google Profile, Picasa Web Albums, Web History,[2] and You Tube.

18. Because the individual using this email account is purporting to sell hosting services for individuals for online gambling and phishing sites, I also request that Google provide a list of all webpages visited by the individual who uses this email address, to the extent this information is stored by Google.

19. On March 15, 2013, I caused a preservation letter pursuant to 18 U.S.C. 2703(f) to be sent to Google, Inc., asking it to preserve the contents of the runningparrots@gmail.com account as of that date for a time period of ninety days. In general, I am also aware that an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for a certain period of time.

BACKGROUND CONCERNING E-MAIL

20. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google allows subscribers to obtain e-mail accounts at the domain name googlemail.com like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications

[2] Google Web History stores information related to search queries entered into Google, the results that appeared, and the pages visited, including the URL (website address).

(including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

22. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

23. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account

(such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

24. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.